360TI-SV-2019-0009 WinRAR 远程代码执行漏洞（CVE-2018-20250）通告

文档信息

编号	360TI-SV-2019-0009
关键字	CVE-2018-20250 WinRAR ACE
发布日期	2019 年 2 月 21 日
更新日期	2019 年 2 月 21 日
TLP	WHITE
分析团队	360 威胁情报中心

通告背景

WinRAR 是一款流行的解压缩工具，据其官网上发布的数据，全球有超过 5 亿的用户在使用 WinRAR。

2019 年 2 月 20 日，安全厂商 checkpoint 发布了名为<<Extracting a 19 Year Old Code Execution from WinRAR>>的文章（见参考[1]），文章披露了一个存在于 WinRAR 中用于 ace 文件解析的 DLL 模块中的绝对路径穿越漏洞，可导致远程代码执行。

360 威胁情报中心经过测试确认该攻击方法可用，由于 WinRAR 工具的安装量较大，且大多数用户疏于对该工具的更新，360 威胁情报中心特此通告提醒用户和企业尽快采取必要防御应对措施以保障终端的安全。

漏洞概要

漏洞名称	WinRAR 绝对路径穿越漏洞				
威胁类型	远程代码执行	**威胁等级**	高	**漏洞 ID**	CVE-2018-20250
漏洞利用条件					
将压缩包解压到当前文件夹便会触发漏洞（对压缩包所在目录有要求）					
漏洞利用场景					
通过鱼叉邮件或者社交渠道进行攻击					
受影响系统及应用版本					
WinRAR 5.70 bate1 之前的版本，以及使用了 UNACEV2.dll 模块的压缩软件					
不受影响影响系统及应用版本					
WinRAR 5.70 bate1					

漏洞描述

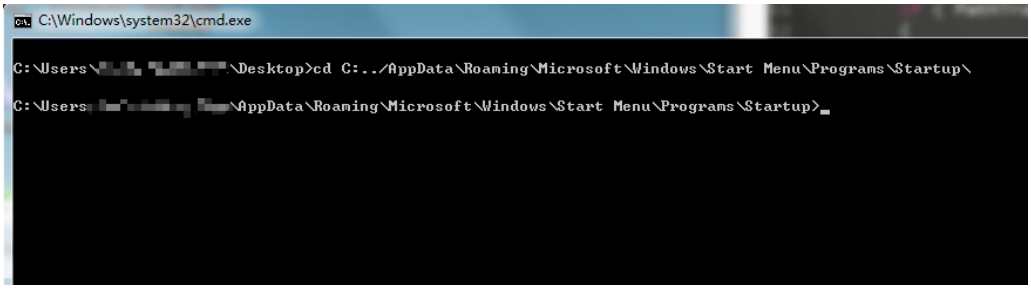
WinRAR 是一款流行的解压缩工具，2019 年 2 月 20 日，安全厂商 checkpoint 发布了名为<<Extracting a 19 Year Old Code Execution from WinRAR>>的文章，文章披露了一个存在于 WinRAR 中用于 ace 文件解析的 DLL 中的绝对路径穿越漏洞，可导致远程代码执行。

漏洞原理

该漏洞是由于与 ace 处理相关的 DLL 在对解压目标的相对路径（filename）进行解析时，由于 CleanPath 函数过滤路径不严格导致：

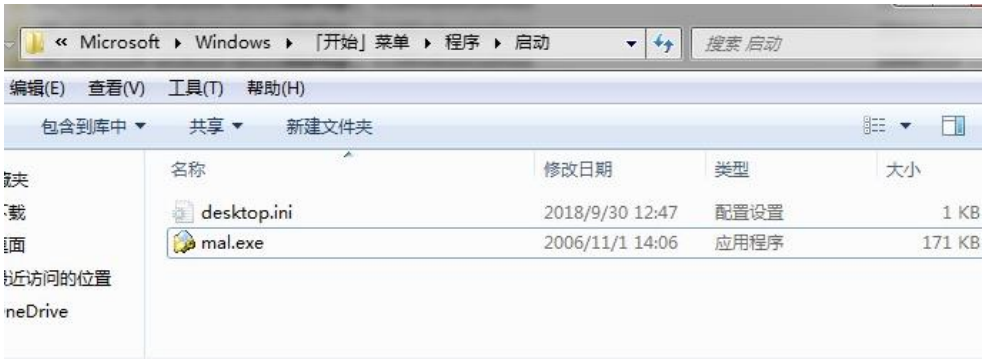
```
1  BOOL CleanPath(PCHAR Path)
2  {
3     char *PathTraversalPos = NULL
4     if ( Path[1] == ':' && Path[2] == '\\' ) Step1
5       strcpy(Path, &Path[3]);
6     if ( Path[1] == ':' && Path[2] != '\\' ) Step2
7       strcpy(Path, &Path[2]);
8     PathTraversalPos = strstr(Path, "..\\");Step3
9     while ( PathTraversalPos )
10    {
11        if ( PathTraversalPos == Path || *(PathTraversalPos - 1) == '\\' )
12        {
13          strcpy(Path, &Path[3]);
14          PathTraversalPos = strstr(Path, "..\\");
15        }
16        else
17        {
18          PathTraversalPos = strstr(Path + 1, "..\\");
19        }
20    }
21  return Path
22 }
```

如针对以下路径：
C:\C:C:../AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\some_file.exe
调用这个函数后 CleanPath(“C:\C:C:../AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\some_file.exe”)
经过 Step1：
C:C:../AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\some_file.exe
经过 Step2：
C:../AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\some_file.exe
经过 Step3：
此时因为 C:之后使用的是“../”不是“..\”，所以不会进入 while 循环，直接返回。
最后返回的结果为：
C:../AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\some_file.exe
这个路径可以直接实现路径穿越：



利用还原

按照 checkpoint 文章所述，360 威胁情报中心构造了相关验证代码，将 ace 文件中的 filename 修改之后，解压压缩包到当前目录，此时压缩包中相关内容直接被解压到 Windows 的启动目录，当重启主机后，模拟恶意软件的 mal.exe 将自启动。



该漏洞通常用于将恶意代码直接投递到启动目录，如下所示：
C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

利用条件

当将恶意软件拷贝到启动目录时，存在一定限制
C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
目前来看只能使用一次“../“（主要用于忽略用户名）
在以上要求下，该漏洞依然适用于大多数攻击场景：
如附件拖拽到桌面解压
C:\Users\xxx\Desktop
主流浏览器的下载目录（chrome，firefox，ie）解压
C:\Users\xxxx\Downloads
以下是主要列举的一些易受攻击的目录列表（红色目录，uac 开启的情况下，WinRAR 将无法拷贝）：

容易被利用的敏感目录	路径
启动	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
ProgramFiles	C:\Program Files\
Windows	C:\Windows\

一些主流软件下载目录的利用情况如下:

软件名	启动目录	ProgramFiles目录	Windows目录	默认路径
CHROME\FireFox\IE	√	×	×	C:\Users\<username>\Downloads\
WECHAT	×	×	×	C:\Users\<username>\Documents\WeChat Files\
桌面	√	×	×	C:\Users\<username>\DeskTop\
QQ	×	×	×	C:\Users\<username>\Documents\Tencent Files\<QQID>\FileRecv\

修复方法

1. 目前软件厂商已经发布了最新的 WinRAR 版本，360 威胁情报中心建议用户及时更新升级 WinRAR（5.70 beta 1）到最新版本 https://www.rarlab.com/

2. 如暂时无法安装补丁，可以直接删除漏洞的 DLL（UNACEV2.DLL），这样不影响一般的使用，但是遇到 ace 的文件会报错。

参考资料

[1].https://research.checkpoint.com/extracting-code-execution-from-winrar/